QUADRATIC TWISTS OF PAIRS OF ELLIPTIC CURVES

SIMAN WONG FEBRUARY 2, 2008 – 06 : 35 **DRAFT**

Abstract. Given two elliptic curves defined over a number field K, not both with j-invariant zero, we show that there are infinitely many $D \in K^\times$ with pairwise distinct image in $K^\times/K^{\times 2}$, such that the quadratic twist of both curves by D have positive Mordell-Weil rank. The proof depends on relating the values of pairs of cubic polynomials to rational points on another elliptic curve, and on a fiber product construction.

1. Introduction

Fix two elliptic curves over $\mathbf{Q}$ with coprime conductors. Then the parity conjecture predicts that there are infinitely many square-free integers D so that the quadratic twist of both curves by D have positive Mordell-Weil rank. This argument no longer applies if the curves have opposite root numbers and if their conductors have the same square-free part, not to mention the fact that it is based on a deep conjecture. Furthermore, Rohrlich informed us that there exist number fields K and elliptic curves E over K for which every quadratic twist of E over K has even analytic rank [2]. In this paper we give an unconditional construction of simultaneous positive rank twists under a mild restriction on j-invariants.

Theorem 1. *For any pair of elliptic curves defined over a number field K, not both with j-invariant zero, there exist infinitely many $D \in K^\times$ with pairwise distinct image in $K^\times/K^{\times 2}$, such that the quadratic twist by D of both curves have positive Mordell-Weil rank over K.*

Remark 1. The elements D in the theorem are values of a cubic polynomial at the x-coordinate of multiples of a non-torsion point on another elliptic curve. In particular, they form a thin set, while the parity conjecture when applicable yields a set of positive density.

Apply theorem 1 to the case where one curve in the pair is the quadratic twist of the other one and we deduce the following result.

Corollary. *Let E be an elliptic curve defined over a number field K with non-zero j-invariant. Then for any $\delta \in K^\times$, there exist infinitely many $D \in K^\times$ with pairwise distinct image in $K^\times/K^{\times 2}$, such that the quadratic twist of E by both D and $D\delta$ have positive Mordell-Weil rank over K.* □

Remark 2. In general we do not know that the elements D furnished by the corollary are coprime to δ. This extra requirement does hold trivially when δ is irreducible.

1991 *Mathematics Subject Classification.* Primary 11G05.

Key words and phrases. Elliptic curve, fiber product, rank, quadratic twist.

In the case of j-invariant zero we have the following partial result.

Theorem 2. *Let E_1, E_2 be elliptic curves defined over a number field K with j-invariant zero. Then there exists $\lambda \in K^\times$ such that, if we denote by E_i' the sextic twist of E_i by λ, then there are infinitely many $D \in K^\times$ with pairwise distinct image in $K^\times/K^{\times 2}$, such that the quadratic twist by D of both E_1' and E_2' have positive Mordell-Weil rank over K.*

At most finitely many quadratic twists of a fixed elliptic curve over K has K-rational torsion points of order > 2. To find positive rank twists of $y^2 = f(x)$ it then suffices to find $x_0 \in K$ so that $f(x_0) \in K - K^2$. Given another elliptic curve $y^2 = g(x)$, to find simultaneous positive rank twists for both curves we are then led to seek conditions on f and g so that

(i) the cubic equation $f(x) = g(y)$ defines another elliptic curve E'/K;
(ii) we can construct a point P' of infinite order on $E'(K)$; and
(iii) we evaluate $f(x) = g(y)$ at multiples of P' to generate infinitely many values with pairwise distinct image in $K^\times/K^{\times 2}$.

The solutions to $f(x) = g(y)$ for which this common value has a given image $\lambda \in K^\times/K^{\times 2}$ turn out to be parameterized by a certain fiber product C_λ of elliptic curves; Step (iii) then comes down to showing that every C_λ has geometric genus > 1. As for Step (ii), the cubic equation $f(x) = g(y)$ contains several natural solutions if at least one of $y^2 = f(x)$ and $y^2 = g(x)$ has non-zero j-invariant, but we need to show that these points give rise to non-torsion points on $E'(K)$. We do that by adjusting the Weierstrass models of the curves.

We expect theorem 1 to hold with no restriction on j-invariant. Removing this condition, however, seems non-trivial, cf. Remark 3. Similarly, theorem 1 should hold for any finite collection of elliptic curves, but our argument does not generalize to this setup.

2. A fiber product

Given a pair $(a, b) \in K^2$ with $4a^3 + 27b^2 \neq 0$, let $f_{a,b}(x) = x^3 + ax + b$, and denote by $E_{a,b}$ the elliptic curve over K defined by the Weierstrass equation $y^2 = f_{a,b}(x)$. Given two such pairs $(a, b), (c, d)$, denote by $E' = E'_{a,b,c,d}$ the projective plane curve over K defined by

$$z^3 f_{a,b}(x/z) = z^3 f_{c,d}(y/z). \tag{1}$$

It contains the rational point $[x : y : z] = [1 : 1 : 0]$ and, provided that $a \neq c$, another point $P' = P'_{a,b,c,d} = [b-d : b-d : c-a]$. In the next section we will study conditions under which E' is non-singular and for which P' is a non-torsion point. For the rest of this section we will investigate Step (iii), but we should point out that P' becomes $[1 : 1 : 0]$ when $c - a = 0$. This happens notably when $a = c = 0$, i.e. when both curves have j-invariant zero, and this turns out to be the source of the restriction on j-invariant in the theorem. If we try to generalize (1) by using $z^3 f_{a,b}(x/z) = \mu^2 z^3 f_{c,d}(y/z)$, the new equation seems to have no natural rational point unless μ is a perfect cube, in which case we are essentially back to (1).

Denote by E_λ the twisted elliptic curve $\lambda y^2 = f_{a,b}(x)$, and by $\varphi_\lambda : E_\lambda \to \mathbf{P}^1$ the projection defined by the affine map $(x, y) \mapsto x$. Denote by $\psi : E' \to \mathbf{P}^1$ the projection given on the affine curve $f_{a,b}(x) = f_{c,d}(y)$ by $(x, y) \mapsto x$. Denote by C_λ/K the fiber product $E_\lambda \times_{\mathbf{P}^1} E'$ defined via φ_λ and ψ. This is a projective curve over K, and it has infinitely many K-rational

points precisely if there are infinitely many pairs $(x_0, y_0) \in K^2$ such that the common value $f(x_0) = g(y_0)$ is λ times a perfect square in K. To handle Step (iii) it then suffices to show that every C_λ has geometric genus > 1 (we will clarify this in the proof of theorem 1).

Lemma 1. *Let (a, b) and (c, d) be as above. If E' is non-singular and if $\lambda \neq 0$, then the fiber product C_λ is non-singular and has genus > 1.*

Proof. The branched locus of φ_λ consists precisely of the roots of $f_{a,b}(x)$ (where as usual we view $\overline{K}$ as $\mathbf{A}^1_{\overline{K}} \subset \mathbf{P}^1_{\overline{K}}$) plus the point $\infty \in \mathbf{P}^1$. The fiber of ψ above ∞ consists of those solutions to (1) with $z = 0$; there are three distinct ones, so the triple cover ψ is not branched over ∞. Now, ψ is ramified above a finite point $x_0 \in \overline{K}$ precisely when $f_{c,d}(y) - f_{a,b}(x_0)$, as a cubic polynomial in y, is not separable. This is equivalent to $4c^3 + 27(d - f_{a,b}(x_0))^2 = 0$. Since $f_{c,d}$ is separable, it means that $f_{a,b}(x_0) \neq 0$. Thus the branched loci of φ_λ and ψ are disjoint. Furthermore, E' and $E_{a,b}$ are both non-singular, so the fiber product C_λ is also non-singular. To compute its genus we can then apply the Riemann-Hurwitz formula.

Denote by $\pi : C_\lambda \to \mathbf{P}^1$ the projection coming from the fiber product. We saw that the double cover φ_λ is branched above four points in $\mathbf{P}^1$ (since $f_{a,b}$ is separable), and that the triple cover ψ is unramified above each of these points. This gives 12 points on $C_\lambda(\overline{K})$ at which π has ramification index 2. By the Riemann-Hurwitz formula, the ramification of π above the branched points of φ_λ alone implies that C_λ has genus ≥ 1. But ψ and φ_λ have disjoint branched loci, so π has additional ramification, whence C_λ must have genus > 1. $\square$

3. Non-torsion points

We begin with a criterion for $E'_{a,b,c,d}$ to be non-singular. Using the command `Weierstrassform` in the computer algebra system `MAPLE`, we find that the transformation

$$\begin{aligned} X &= 3x^2 + a + 3yx + 3y^2 + c \\ Y &= -3ya - 6ax - 3cx - 9b/2 + 3cy + 9d/2 - 9yx^2 - 9y^2x - 9x^3 \end{aligned} \tag{2}$$

takes $f_{a,b}(x) = f_{c,d}(y)$ to

$$E'' : Y^2 = X^3 - 3acX - a^3 - c^3 - 27(b - d)^2/4 \tag{3}$$

(actually (2) is the negative of that furnished by `MAPLE`; we make this adjustment so that E'' takes on the usual Weierstrass form). Under this transformation, the point $P'_{a,b,c,d}$ becomes

$$P'' = P''_{a,b,c,d} = \Big(\frac{9(b-d)^2 + (a-c)^2(a+c)}{(a-c)^2},\ \frac{9(b-d)(6(b-d)^2 + (a-c)^2(a+c))}{2(a-c)^3} \Big) \tag{4}$$

(we will address the vanishing of $a - c$ later on). So if the discriminant of the cubic on the right side of (3), namely

$$108a^3c^3 - 27(4a^3 + 4c^3 + 27(b-d)^2)^2/16, \tag{5}$$

is non-zero, then E'' is an elliptic curve, and hence so does E'. Note that these `MAPLE` computations are purely symbolic and hence applies to all sufficiently large characteristics.

For any number field k, denote by $\mathcal{O}_k$ the ring of integers of k, and by $\mathbf{F}_\mathfrak{p}$ the residue field of $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_k$. For any $u \in K^\times$, we write $\mathfrak{p} \nmid u$ if u is a $\mathfrak{p}$-adic unit.

Lemma 2. *Given two elliptic curves over K which are not isomorphic over K and not both with j-invariant zero, we can find Weierstrass equations $E_{a,b}$ and $E_{c,d}$ for them so that $E''_{a,b,c,d}$ is an elliptic curve, and that $P''_{a,b,c,d}$ is a non-torsion point in $E''_{a,b,c,d}(K)$.*

Proof. Fix Weierstrass equations $E_{a,b}$ and $E_{c,d}$ for these two curves. Without loss of generality, suppose $E_{a,b}$ has non-zero j-invariant; equivalently, $a \neq 0$.

First, suppose $b = 0$. Fix $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ with $\mathfrak{p} \nmid 6a$, and fix a non-zero element $\pi \in \mathfrak{p}$. Set $\overline{c} = \pi^4 c$ and $\overline{d} = \pi^6 d$. Then $E_{\overline{c},\overline{d}}$ defines the same elliptic curve over K as $E_{c,d}$, and

- the discriminant of $E''_{a,b,\overline{c},\overline{d}}$ is non-zero modulo $\mathfrak{p}$, so $E''_{a,b,\overline{c},\overline{d}}$ is non-singular over $\mathbf{F}_\mathfrak{p}$, and hence over K;
- $a \not\equiv \overline{c} \pmod{\mathfrak{p}}$, so $P''_{a,b,\overline{c},\overline{d}}$ is well-defined over $\mathbf{F}_\mathfrak{p}$, and hence over K; and
- $P''_{a,b,\overline{c},\overline{d}}$ is a 2-torsion point in $E''_{a,b,\overline{c},\overline{d}}(\mathbf{F}_\mathfrak{p})$ but not in $E''_{a,b,\overline{c},\overline{d}}(K)$.

Apply Merel's theorem on torsion points [1] and we see that, providing that the residual characteristic of $\mathfrak{p}$ is large enough (depending on K), $P''_{a,b,\overline{c},\overline{d}}$ is a non-torsion point in $E''_{a,b,\overline{c},\overline{d}}(K)$. A similar argument covers the case $d = 0$. For the rest of the proof we will take $bd \neq 0$.

Lemma 3. *Suppose $bd \neq 0$. Then lemma 2 would follow if there exists a $\lambda \in K^\times$ and $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ not dividing $6, a, b, d$ and $4a^3+27b^2$, such that $b \equiv \lambda^6 d \pmod{\mathfrak{p}}$ and $a \not\equiv \lambda^4 c \pmod{\mathfrak{p}}$ (in which case $\mathfrak{p} \nmid \lambda$ as well).*

Proof of Lemma 3. With $\mathfrak{p}$ and λ as above, set $\overline{c} = \lambda^4 c$ and $\overline{d} = \lambda^6 d$. The hypothesis $\mathfrak{p} \nmid 6(4a^3 + 27b^2)$ means that the discriminant of $E''_{a,b,\overline{c},\overline{d}}$ is non-zero modulo $\mathfrak{p}$, so $E''_{a,b,\overline{c},\overline{d}}$ is non-singular over $\mathbf{F}_\mathfrak{p}$, and hence over K. This conclusion remains true if we replace λ by $\lambda + \pi$ for any $\pi \in \mathfrak{p}$. So we can choose π so that

$$a \neq \overline{c}, \quad b \neq \overline{d}, \quad \text{and} \quad 6(b - \overline{d})^2 + (a - \overline{c})^2(a + \overline{c}) \neq 0. \tag{6}$$

The first two conditions above imply that $P''_{a,b,\overline{c},\overline{d}}$ is well-defined over K, and the last condition says that it is not a 2-torsion point in $E''_{a,b,\overline{c},\overline{d}}(K)$. Since $b \equiv \overline{d} \pmod{\mathfrak{p}}$ and $\mathfrak{p} \nmid 2a$, from (4) we see that this point reduces to a point of order 2 in $E''_{a,b,\overline{c},\overline{d}}(\mathbf{F}_\mathfrak{p})$. Apply Merel's theorem as before we see that $P''_{a,b,\overline{c},\overline{d}}$ is not a torsion point in $E''_{a,b,\overline{c},\overline{d}}(K)$. □

Set $\alpha = c/a$ and $\beta = d/b$; the congruence condition in lemma 3 can then be written as

$$\beta \equiv \lambda^6 \pmod{\mathfrak{p}} \text{ and } \alpha \not\equiv \lambda^4 \pmod{\mathfrak{p}}. \tag{7}$$

Suppose there exist $\lambda, \mu \in K$ such that $\beta = \lambda^6$ and $\alpha = \mu^4$. Since $E_{a,b}$ and $E_{c,d}$ are not K-isomorphic, [3, p. 49] implies that $\lambda^4 \neq \mu^4$, whence (7) is satisfied by any $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ with $\mathfrak{p} \nmid (\lambda^4 - \mu^4)$. From now on we will therefore assume that at least one of $K_\alpha = K(\alpha^{1/4})$ or $K_\beta = K(\beta^{1/6})$ is a non-trivial extension of K. To finish the proof of the lemma, we consider three cases based on conditions on K_α and K_β. In two cases the condition (7) will be satisfied so lemma 3 is applicable[1]; in the third case we need to proceed differently.

Case I: $K_\alpha \subsetneq K_\beta$

[1] in what follows, when we can find $\mathfrak{p}$ satisfying (7) we can find infinitely many of them, so the additional non-divisibility condition in lemma 3 is not an issue. We will also assume without further comment that every $\mathfrak{p}$ in what follow to be unramified in K_α/K and in K_β/K.

Spec $\mathcal{O}_{K_\beta}$ has infinitely many $\mathcal{P}$ of degree 1 over K (i.e. its K_β/K-norm is in Spec $\mathcal{O}_K$); for any such $\mathcal{P}$, the congruence $x^6 \equiv \beta \pmod{\mathcal{P}}$ is solvable in $\mathcal{O}_K$. And if for infinitely many such $\mathcal{P}$, some $\mathcal{O}_K$-solution of this congruence is also congruent modulo $\mathcal{P}$ to a root in K_α of $x^4 = \alpha$, say $\alpha_1 \in K_\alpha$, then α_1 would be an actual sixth root of β, contradicting $K(\alpha_1) \subset K_\alpha \subsetneq K_\beta = K(\beta^{1/6}) \subset K(\alpha_1)$. So for infinitely many $\mathcal{P} \in$ Spec $\mathcal{O}_{K_\beta}$ of degree 1 over K, we can find $\lambda \in \mathcal{O}_K$ (depending on $\mathcal{P}$) such that $\beta \equiv \lambda^6 \pmod{\mathcal{P}}$ and $\alpha \not\equiv \lambda^4 \pmod{\mathcal{P}}$. Both sides of each of these two congruences are in K, so we can change the modulus from $\mathcal{P}$ to $\mathcal{P} \cap \mathcal{O}_K$, which is in Spec $\mathcal{O}_K$ since $\mathcal{P}$ has degree 1 over K, and (7) follows.

Case II: $K_\alpha \not\subset K_\beta$

If L_β, the Galois closure of K_β/K, does not contain K_α, then it does not contain the Galois closure of K_α/K either, in which case we can find infinitely many $\mathfrak{p} \in$ Spec $\mathcal{O}_K$ such that Spec $\mathcal{O}_{K_\beta}$ has a degree 1 prime lying above $\mathfrak{p}$, but Spec $\mathcal{O}_{K_\alpha}$ does not. Once $\mathfrak{p}$ is chosen, λ as in (7) follows as above.

Now, suppose $K_\alpha \subset L_\beta$. Since $[K_\beta : K]$ divides 6, from $K_\alpha \not\subset K_\beta$ and $K_\alpha \subset L_\beta$ we see that $[K_\beta : K] = 3$ or 6. If $[K_\beta : K] = 3$, then L_β/K is a dihedral extension of degree 6; since $[K_\alpha : K]$ divides 4, that means K_α is the unique quadratic subfield of L_β. Let $\mathfrak{p} \in$ Spec $\mathcal{O}_K$ be unramifed in L_β, and that its Frobenius conjugacy class is the class of order 2 elements in Gal(L_β/K). Then $\mathfrak{p}$ is inert in K_α, and $\mathcal{O}_{K_\beta}$ has a maximal ideal $\mathcal{P}$ of degree 1 lying above $\mathfrak{p}$. That means $\alpha \not\equiv \lambda^4 \pmod{\mathfrak{p}}$ for any $\lambda \in \mathcal{O}_K$, while $\beta \equiv \lambda^6 \pmod{\mathcal{P}}$ has a solution in $\mathcal{O}_K$. As before we can replace $\mathcal{P}$ by $\mathfrak{p}$, so the condition (7) is satisfied.

Next, suppose $K_\alpha \subset L_\beta$ and $[K_\beta : K] = 6$. If K_β/K is Galois, then from $[K_\alpha : K]$ dividing 4 we see that K_α/K is quadratic, and the argument in the paragraph above applies. Now, suppose K_β/K is not Galois, which happens if and only if $\sqrt{-3}$ is not in K_β. That means K'_β, the unique cubic subfield $K(\beta^{1/3})$ of K_β, is not Galois; denote by L'_β/K its Galois closure. This is a diheral extension of degree 6, and its unique quadratic subfield is not $K(\sqrt{\beta})$, otherwise K_β/K would be Galois. Thus $L'_\beta \cap K(\sqrt{\beta}) = K$ and of course $L_\beta = L'_\beta(\sqrt{\beta})$, so

$$\mathrm{Gal}(L_\beta/K) \simeq \mathrm{Gal}(L'_\beta/K) \times \mathrm{Gal}(K(\sqrt{\beta})/K).$$

Denote by γ the conjugacy class of elements of Gal(L_β/K) that projects to the class of order 2 elements in Gal(L'_β/K) and to the trivial class in Gal$(K(\sqrt{\beta})/K)$. Then for any $\mathfrak{p}_\gamma \in$ Spec $\mathcal{O}_K$ which is unramifed in L_β and whose Frobenius conjugacy class in Gal(L_β/K) is γ, there is a maximal ideal in each of Spec $\mathcal{O}_{K'_\beta}$ and Spec $\mathcal{O}_{K(\sqrt{\beta})}$ of degree 1 over K lying above $\mathfrak{p}_\gamma$, but $\mathfrak{p}_\gamma$ does not split completely in the unique quartic subfield of L_β/K. The first statement means that $\beta \equiv \lambda^6 \pmod{\mathfrak{p}_\gamma}$ has a solution in $\mathcal{O}_K$. We claim that the second statement means that Spec $\mathcal{O}_{K_\alpha}$ has no maximal ideal of degree 1 over K lying above $\mathfrak{p}_\gamma$, in which case $\alpha \not\equiv \lambda^4 \pmod{\mathfrak{p}_\gamma}$ has no solution in $\mathcal{O}_K$, and the condition (7) is satisfied.

Note that $[K_\alpha : K]$ divides 4 and $K_\alpha \not\subset K_\beta$, so $[K_\alpha : K] = 4$ or 2. If $[K_\alpha : K] = 4$, then K_α is the unique quartic subfield of L_β, and hence Galois; the claim then follows immediately from our earlier observation that $\mathfrak{p}_\gamma$ does not splitting completely in K_α/K. If $[K_\alpha : K] = 2$, from $K(\sqrt{\beta}) \subset K_\beta$ and $K_\alpha \subset L_\beta$ we see that $K_\alpha \neq K(\sqrt{\beta})$, so $\mathfrak{p} \in$ Spec $\mathcal{O}_K$ is inert in K_α/K if and only if its Frobenius in Gal(L'_β/K) is the unique class of order 2 elements. Recall the definition of $\mathfrak{p}_\gamma$ and we are done.

Case III: $K_\alpha = K_\beta$

Since $[K_\alpha : K]$ divides 4, $[K_\beta : K]$ divides 6, and since at least one of K_α, K_β is a non-trivial extension of K, that means $K_\alpha = K_\beta$ is a quadratic extension of K. Consequently, $\alpha = \alpha_0^2$ and $\beta = \beta_0^3$ for some $\alpha_0, \beta_0 \in K$, with $K(\sqrt{\beta_0}) = K(\sqrt{\alpha_0}) \neq K$; the equality means that $\beta_0 = \alpha_0\alpha_1^2$ for some $\alpha_1 \in K$, and the inequality means that $\alpha_0 \in K$ is not a square. Note that $\alpha_1 = 1$ corresponds precisely to the case where the two curves are non-trivial quadratic twists of one another.

Set $\overline{c} = \lambda^4 c/\alpha_1^4 = a\alpha_0^2\lambda^4/\alpha_1^4$ and $\overline{d} = \lambda^6 d/\alpha_1^6 = b\alpha_0^3\lambda^6$. Then $E_{c,d}$ and $E_{\overline{c},\overline{d}}$ are isomorphic over K, and

$$\begin{aligned} \overline{d} - b &= b(\alpha_0^3\lambda^6 - 1) &&= b(\alpha_0\lambda^2 - 1)((\alpha_0\lambda^2)^2 + \alpha_0\lambda^2 + 1), \\ \overline{c} - a &= a\Big(\frac{\alpha_0^2\lambda^4}{\alpha_1^4} - 1\Big) &&= \frac{a(\alpha_0\lambda^2 - \alpha_1^2)(\alpha_0\lambda^2 + \alpha_1^2)}{\alpha_1^4}. \end{aligned}$$

Since $\alpha_0 \in K$ is not a square, $\alpha_0\lambda^2 - 1$ viewed as a polynomial in λ is K-irreducible. Thus

$$\{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K : \ \nu_\mathfrak{p}(\alpha_0\lambda^2 - 1) \text{ is positive for some } \lambda \in \mathcal{O}_K\}$$

is infinite, where $\nu_\mathfrak{p}$ denotes an additive $\mathfrak{p}$-adic valuation for $\mathcal{O}_K$. Choose $\mathfrak{p} \in S$ for which

$$a, \alpha_0, \alpha_1, \alpha_0^2 \pm 1, \alpha_1^4 - 1 \text{ and } \alpha_1^{12} - 1 \tag{8}$$

are all $\mathfrak{p}$-adic units, and pick a $\lambda \in \mathcal{O}_K$ (depending on $\mathfrak{p}$) so that $\nu_\mathfrak{p}(\alpha_0\lambda^2 - 1) > 0$. Then

(i) $\overline{c} \not\equiv a \pmod{\mathfrak{p}}$ since $\nu_\mathfrak{p}(\alpha_0^2 \pm 1) = 0$;
(ii) $\overline{d} \equiv b \pmod{\mathfrak{p}}$ since $\nu_\mathfrak{p}(\alpha_0\lambda^2 - 1) > 0$; and
(iii) $\overline{d} \neq b$ for all but finitely many $\mathfrak{p}$.

From (i) we see that $P''_{a,b,\overline{c},\overline{d}}$ is well-defined over $\mathbf{F}_\mathfrak{p}$, and hence over K. Its Y-coordinate is zero modulo $\mathfrak{p}$, by (ii), but is non-zero in K for all but finitely many $\mathfrak{p}$, by (iii). By (ii), the discriminant (5) of $E''_{a,b,\overline{c},\overline{d}}$ is congruent modulo $\mathfrak{p}$ to $-27(a-\overline{c})^2(a^2 + a\overline{c} + \overline{c}^2)^2$. We saw that $a - \overline{c} \not\equiv 0 \pmod{\mathfrak{p}}$, and since $\alpha_0\lambda^2 \equiv 1 \pmod{\mathfrak{p}}$,

$$a^2 + a\overline{c} + \overline{c}^2 = a^2\Big(1 + \Big(\frac{\alpha_0^2\lambda^4}{\alpha_1^4}\Big) + \Big(\frac{\alpha_0^2\lambda^4}{\alpha_1^4}\Big)^2\Big) \equiv \frac{a^2}{\alpha_1^8}\frac{1 - \alpha_1^{12}}{1 - \alpha_1^4} \pmod{\mathfrak{p}},$$

which by (8) is a $\mathfrak{p}$-adic unit. Thus $E''_{a,b,\overline{c},\overline{d}}$ is non-singular over $\mathbf{F}_\mathfrak{p}$, and hence over K. Our earlier comment about the Y-coordinate of $P''_{a,b,\overline{c},\overline{d}}$ means that this point does not have order 2 in $E''_{a,b,\overline{c},\overline{d}}(K)$ but reduces to a point of order 2 modulo $\mathfrak{p}$. Apply Merel's theorem as before and we see that $P''_{a,b,\overline{c},\overline{d}}$ is non-torsion in $E''_{a,b,\overline{c},\overline{d}}(K)$. □

4. Proof of the Theorems

Proof of Theorem 1. If the two elliptic curves in theorem 1 are isomorphic over K, then the desired positive rank twists follow readily from, for example, the elementary construction mentioned after the statement of theorem 2. So suppose they are not isomorphic over K, in which case lemma 2 furnishes Weierstrass models $E_{a,b}$ and $E_{\overline{c},\overline{d}}$ for them, such that $E''_{a,b,\overline{c},\overline{d}}$ is non-singular and contains a non-torsion rational point $P''_{a,b,\overline{c},\overline{d}}$. That means $P'_{a,b,\overline{c},\overline{d}}$ is a non-torsion point on $E'_{a,b,\overline{c},\overline{d}}$. For every integer k, denote by x_k and y_k the x- and y-coordinate

of $kP'_{a,b,\overline{c},\overline{d}}$. Then (x_k, y_k) is a rational solution to $f_{a,b}(x) = f_{\overline{c},\overline{d}}(y)$ for every k. Denote by $z_k \in K$ this common value $f_{a,b}(x_k) = f_{\overline{c},\overline{d}}(y_k)$. It is zero for at most finitely many k, so for all sufficiently large k, each elliptic curve $z_k y^2 = f_{a,b}(x)$ and $z_k y^2 = f_{\overline{c},\overline{d}}(y)$ has a rational point with non-zero y-coordinate. At most finitely many quadratic twists of any elliptic curve over K has K-rational torsion points of order > 2, so the two twisted curves above have positive Mordell-Weil rank over K. By lemma 1, for any $\lambda \in K^\times$ there are at most finitely many k for which z_k is λ times a perfect square-free in K, and the theorem follows. □

Proof of Theorem 2. To say that both curves have j-invariant zero is to say that $a = c = 0$. If in addition $b = d$, then the two curves are identical, in which case the theorem follows readily from the elementary construction mentioned in the introduction. So from now on assume that $b \neq d$, in which case $E''_{0,b,0,d}$ becomes $E''' : Y^2 = X^3 - 27(b-d)^2/4$. The point P' becomes $[1:1:0]$, which under the `MAPLE` transformation is the point at infinity for E'''. In general E''' has no other K-rational point, so our argument above fails to generate a single quadratic twist, let alone infinitely many, for which both $E_{0,b}$ and $E_{0,d}$ have positive rank. On the other hand, we claim that there are infinitely many $\lambda \in K$ whose image in $K^\times/K^{\times 3}$ are pairwise distinct, such that the cubic twist of $E''_{0,b,0,d}$ by λ has positive Mordell-Weil rank. Since this cubic twist can be written as $Y^2 = X^3 - 27(\lambda b - \lambda d)^2/4$, that means $E''_{0,\lambda b,0,\lambda d}$ has positive rank. We can now resume the argument in the last paragraph of the proof of theorem 1 for the pair of sextic twists $E_{0,\lambda b}$ and $E_{0,\lambda d}$ (which only requires the *existence* and not the explicit description of a non-torsion point on $E''_{0,\lambda b,0,\lambda d}$) and theorem 2 follows.

It remains to verify the claim. The cubic twist $Y^2 = X^3 - 27(\lambda b - \lambda d)^2/4$ is equivalent to $U^3 - V^3 = 4\lambda(d-b)$. Write λ as $16(d-b)^2 t$ and we are reduced to show that $E_t : U^3 - V^3 = t$ has positive rank for infinitely many t whose image in $K^\times/K^{\times 3}$ are pairwise distinct. Since the E_t are cubic twists, they have trivial torsion for all but finitely many such t, so it suffices to show that E_t has a non-trivial rational point for infinitely many t whose image in $K^\times/K^{\times 3}$ are pairwise distinct. We proceed inductively as follow. Pick $\mathfrak{p} \nmid 3$ in $\operatorname{Spec} \mathcal{O}_K$. Since $U^3 - V^3 = (U-V)(U^2 + UV + V^2)$, if we choose $u, v \in \mathcal{O}_K$ such that $u \equiv (p+1) \pmod{p^2}$ and $v \equiv 1 \pmod{p^2}$, then $\mathfrak{p} || (u^3 - v^3)$. Thus $u^3 - v^3$ could serve as one of the desired t values. Now, suppose we have constructed finitely many such values $t_1, \ldots, t_m$. Repeat the process with a new $\mathfrak{p}_{m+1} \nmid (t_1 \cdots t_m)$ and we obtain a new t_{m+1}; the conditions $\mathfrak{p}_{m+1} || t_{m+1}$ and $\mathfrak{p}_{m+1} \nmid (t_1 \cdots t_m)$ mean that the cube-free part of t_{m+1} is different from those of the other t_i. Continue this process and we are done. □

Remark 3. If we try to treat the remaining case of theorem 1 directly, we need to show that for infinitely many square-free integers D, the system

$$(\gamma + \delta\sqrt{D})^3 + b - (\alpha + \beta\sqrt{D})^2 \;=\; 0 \;=\; (\gamma' + \delta'\sqrt{D})^3 + d - (\alpha' + \beta'\sqrt{D})^2$$

has a rational point $(\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta')$. View each of the two equations above as the vanishing of an algebraic integer in $\mathcal{O}_K[\sqrt{D}]$, eliminate the variables α, α' and D and we arrive at a family of curves of geometric genus 11 in the variables γ, γ' over the affine parameters $\beta, \beta', \delta, \delta'$. Showing that the total space of such a family has one rational point, let alone infinitely many, with $bd \neq 0$ seems highly non-trivial.

If K contains a primitive third root of unity ζ_3, then the projective curve $E_{a,b,c,d}$ acquires the additional K-rational points $[1 : \zeta_3 : 0]$ and $[1 : \zeta_3^2 : 0]$. However, when $a = c = 0$ we check that these become 2-torsion points on $E_{a,b,c,d}(K)$, and hence they cannot be use to generate an infinite collection of positive rank twists over K.

Acknowledgment. Part of this work was carried out during the Banff workshop on analytic methods on diophantine equations. We would like to thank to the organizers for providing a conducive working environment, and Professors Hajir, Rohrlich and Rosen for useful discussion. This research is supported in part by NSA grant H98230-05-1-0069.

References

[1] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124** (1996) 437-449.
[2] D. E. Rohrlich, Email communication. June 2006.
[3] J. H. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

Department of Mathematics & Statistics, University of Massachusetts. Amherst, MA 01003-9305 USA

E-mail address: siman@math.umass.edu